CRYPTO PROJECT:
MAINTAINING HEALTH RECORDS USING BLOCKCHAIN PRINCIPLES

If we run the program it initially asks us with four options.
1,2,3,4

1)If we want to create a new user we will use this option.For the time being we use a file from which we take input if we want to create a new user.
It has five users in it.We can update it in the future if we want to add more users.We can also take the input from the terminal if we want to do so.
For each user entry a block is mined and the details are put into it.The fields a user contains are.His Name(In Encrypted Form.But the entry will be in normal format),followed by Medical Report and set of users which can access the data of a particular user to verify him and also Age.
In the Block we also store the previous Hash and current Hash and for the genesis block the prevhash value is Zero.So this option of the code does the creation of a block along with mining it.For the mining part we used SHA_256 Algorithm which always returns a unique 256 bit value for every different input.Here the difficulty for mining the block is set to 3.We can change it in the future if we want to.When we mine the block we generate a key(passcode) which is unique to every user.This is the secret password that user has to keep with himself whenever he wants to access the data or he wants to modify his data.This is the private key kindof thing in this scenario.
2)Option 2 lists the user's information.It displays all the previous information of user if user has made any changes to his info.First it asks to enter a key and then if the key is valid one(Here key is the passcode that is generated while mining the block) then the results will be printed to the block which corresponds to the key given.If the key is invalid it says that key is invalid.
3)This option is used when the user wants to update his details.When ever user wants to update his details his passcode should be entered and if it is valid it asks the user to enter the details that he wants to update.Remember that the user cant update his Name field.So whenever he enters his details for the first time he should enter the correct ones.User should take care of it.Also note that whenever user updates his values he is created a new block and the updated values are added to that block and before that the block is mined.So this also gives us a passcode(new one).This the user should take note of.The user always just needs to keep note of his latest passcode.Because once a new block for him is created all the old passcodes become invalid.
4)This is the verification part.Here in our scenario whenever a user is asked to enter his details there is a field called as Accesible names field where he should enter the encrypted names of the users whom he wants to give access to view his details.So during verification these users have access to view the information and check whether there is any mistake in the entry of the information or not.So for this the person(B) who wants to access the details of other person(A) is prompted to enter his name (Original One) and the name (Encrypted form of the User A).Then we check if there is any entry of B in the accessible names of A.If there is no entry then it says that you are not accessible to view the details.If there is an entry of B in A's details then Zero Knowledge Proof is applied inorder for User A to let know that B has the encrypted name of A and he can view the details.If the Zero knowledge proof result is passed then B is displayed the details of A(All the blocks which contain A's entry in them).Thus verification is done.
Here the parameters for applying Zero Knowledge proof are selecting a large prime number p and generating a generator which generates Zp* elements(g).Then it also asks us to choose any random number from 1 to p-1.And then it asks the verifier to give any number 0 or 1(b).Then according to the values that prover gives to verifier,verifier checks the values.If they match then verifier gives the prover a message saying that Verification part is here and output as YES followed by the details of the user A.

This is the gist of the project.Run it to understand it better.